COURSE CATALOG - IT PROFESSIONAL

JOB FUNCTIONS	AUDIENCES							
	SANS Track 1	SANS Track 2	SANS Track 3	SANS Track 4	SANS Track 5	SANS Track 6	SANS Track 7	SANS Track 9
Laws, Regulations and Policies: Understand government-wide and organization-specific published documents governing mandated requirements and standards for the management and protection of information technology resources.								
Explain and be aware of national and DOE cyber security laws, regulations and procedures								
Ability to lead the effort to ensure security awareness by users and line managers	✓	✓	✓	✓	✓	✓	✓	✓
Ability to draft your organization's cyber security policies	✓	✓					✓	✓
Ability to write and update cyber security procedures	✓	✓					✓	✓
Describe organizational cyber security policies	✓	✓					✓	✓
Recognize and investigate potential violations	✓	✓	✓	✓	✓	✓	✓	✓
Evaluate conflicting functional requirements and select those requirements that will provide the highest level of security at the minimum cost	✓	✓						
Security Program Management: Understand IT security program elements and administrative policies to ensure an effective IT security program.								
Understand the cyber security roles of various organizational personnel	✓			✓			✓	✓
Describe:								
- your organization's internet security procedures	✓						✓	✓
- your organization's network security procedures		✓	✓	✓	✓	✓	✓	✓
- operating system integrity procedures					✓	✓	✓	
- WAN/LAN security procedures	✓	✓	✓	✓	✓	✓	✓	✓
Understand change control policies								
Explain procedural review and updating process								
Define system threats	✓	✓	✓	✓	✓	✓	✓	✓
Define system vulnerabilities	✓	✓	✓	✓	✓	✓	✓	✓
Define the services on his/her systems that are vulnerable and determine whether those services can be turned off	✓	✓			✓	✓	✓	
Describe security inspections/reviews/assessments	✓						✓	✓
Understand system and database integrity	✓	✓	✓	✓	✓	✓	✓	✓
Explain concepts of confidentiality, integrity and accountability	✓			✓		✓		✓
Give examples of alarms, signals and reports						✓	✓	
Describe disaster recovery procedures	✓			✓		✓		
Describe system protection measures:								
- discuss your responsibility for system protection	✓	✓	✓	✓	✓	✓	✓	✓
- describe responsibilities with software copyrights								
- describe protection on software								

JOB FUNCTIONS	AUDIENCES							
	SANS Track 1	SANS Track 2	SANS Track 3	SANS Track 4	SANS Track 5	SANS Track 6	SANS Track 7	SANS Track 9
Security Program Management (continued)								
- describe approaches used to prevent software piracy								
- describe approaches for e-mail privacy	✓							
- describe the use of caller ID								
- describe different types of network security software	✓	✓	✓	✓	✓	✓	✓	✓
- define network firewalls	✓	✓		✓	✓		✓	✓
- define methods of intrusion detection	✓	✓	✓	✓				✓
Describe separation of duties							✓	
Describe continuity planning				✓		✓		
Define an error log		✓	✓	✓	✓	✓	✓	✓
Describe electronic records management	✓	✓					✓	✓
Explain information ownership principles	✓							
Explain how to avoid the five most common social engineering attacks	✓			✓				
Describe authentication mechanisms, discretionary and mandatory access controls, one-time passwords	✓			✓	✓	✓	✓	
Describe password management policy	✓			✓		✓	✓	
Describe configuration management		✓	✓		✓	✓	✓	
Discuss object reuse policy and procedures								
Discuss privileges	✓				✓	✓	✓	
Explain the benefits of auditing and monitoring	✓	✓	✓	✓	✓	✓	✓	✓
Explain risk management concepts	✓				✓	✓	✓	✓
Define categories of risk to an organization and define your organization's risk management process	✓			✓		✓	✓	✓
Design of Security Systems, Processes and Procedures: Provide guidance to ensure safeguards are incorporated in the design of information systems.								
Describe the Project Management Processes								
Design your organization's system and firewall configuration management process, and system architecture including defense in depth approach	✓	✓			✓		✓	✓
Identify integration of location of security components	✓	✓	✓	✓	✓	✓	✓	✓
Design and/or modify the design of cyber security project requirements		✓	✓	✓	✓	✓	✓	✓
Complete implementation strategy and resource estimates for the strategies		✓	✓				✓	✓
Establish requirements for intrusion detection - both for host and network	✓	✓	✓				✓	✓
Participate in the identification of system confidentiality, integrity and availability in relation to user needs and risk management	✓	✓		✓		✓		✓
Draft security concept of operations document for proposed system	✓	✓	✓	✓	✓	✓		✓

JOB FUNCTIONS	AUDIENCES							
	SANS Track 1	SANS Track 2	SANS Track 3	SANS Track 4	SANS Track 5	SANS Track 6	SANS Track 7	SANS Track 9
Development of Security Systems, Processes and Procedures: Ensure that security requirements are considered, resolved and incorporated as information systems and technologies are developed or changed.								
Develop your organization's application development controls	✔	✔	✔	✔	✔	✔	✔	✔
Develop and/or modify security project requirements		✔	✔	✔	✔	✔	✔	✔
Identify and recommend alternative approaches that will satisfy baseline security specifications	✔	✔	✔	✔	✔	✔	✔	✔
Participate in the development and modification of approaches to correct vulnerabilities identified during system implementation	✔	✔	✔	✔	✔	✔	✔	✔
Develop proper system and firewall configuration	✔	✔			✔		✔	
Operation of Security Systems: Implement and maintain systems and their safeguards, identify departures from plans and new vulnerabilities, or make operational and procedural changes, to ensure that appropriate safeguards are within acceptable levels of risk.								
Implement:								
- your organization's configuration management process to ensure that the security concerns identified in the approved plan have been fully addressed	✔	✔	✔	✔	✔	✔	✔	✔
- application development controls	✔	✔	✔	✔	✔	✔	✔	✔
- network security procedures	✔	✔	✔	✔	✔	✔	✔	✔
- operating system integrity procedures	✔				✔			
- WAN/LAN security procedures	✔	✔	✔	✔	✔	✔	✔	✔
Use network access controls as designed	✔	✔	✔	✔	✔	✔	✔	✔
Perform backups	✔	✔			✔	✔	✔	
Perform risk management	✔	✔	✔	✔	✔	✔	✔	✔
Use protection measures	✔	✔	✔	✔	✔	✔	✔	✔
Perform corrective actions	✔	✔	✔	✔	✔			✔
Implement intrusion detection procedures	✔	✔	✔					✔
Use alarms, signals and reports in accordance with existing policies and procedures						✔	✔	
Implement disaster recovery procedures	✔			✔		✔		
Implement storage media protection and controls								
Install virus detection and update virus datasets	✔	✔		✔	✔	✔	✔	✔
Install security patches and test their effectiveness	✔	✔	✔	✔	✔	✔	✔	✔
Develop plans to implement security components	✔	✔	✔	✔	✔	✔	✔	✔
Approve IT security specifications for inclusion in the formal system baseline		✔	✔	✔	✔	✔	✔	✔
Implement programs to address areas of risk for an organization		✔	✔	✔	✔	✔	✔	✔
Institute use of an error log and monitor its use		✔	✔	✔	✔	✔	✔	✔

JOB FUNCTIONS	AUDIENCES							
	SANS Track 1	SANS Track 2	SANS Track 3	SANS Track 4	SANS Track 5	SANS Track 6	SANS Track 7	SANS Track 9
Audit Management: Monitor operational personnel to ensure intended safeguards are in place and have the intended effect.								
Review logs and identify security-related concerns	✓	✓	✓	✓	✓	✓	✓	✓
Identify auditing tools	✓	✓	✓	✓	✓	✓	✓	
Summarize audit-related documentation	✓						✓	
Institute cyber security inspections and policy enforcement	✓						✓	✓
Discuss electronic records management relative to compliance with local policies and procedures							✓	
Monitor systems for accuracy and abnormalities	✓	✓	✓	✓	✓	✓	✓	✓
Demonstrate auditing and monitoring methods	✓	✓	✓		✓	✓	✓	
Identify information resource owners/custodians							✓	
Prepare assessments	✓		✓				✓	
Identify countermeasures applicable to audit trail tampering							✓	
Describe protective measures gained through use of audit trails	✓						✓	
Implement management/oversight change controls							✓	✓
Test and Evaluate Security Systems: Test and evaluate the effectiveness of security safeguards.								
Conduct tests according to established test plan and procedures in a manner that does not alter the program code or compromise security safeguards							✓	
Review IT system development documents for inclusion of appropriate safeguards	✓	✓	✓	✓	✓	✓	✓	✓
Review documents to ensure that the safeguards result in an acceptable level of risk	✓	✓	✓	✓	✓	✓	✓	✓
Provide direction to system developers regarding correction of security problems identified during testing		✓	✓	✓	✓	✓	✓	
Design and develop tests for security safeguard performance under normal operating circumstances and workload levels			✓				✓	
Design and develop tests for security safeguard performance under unusual, improbable circumstances, and ensure that all security related elements will be effectively tested			✓				✓	
Terminate Security Systems: Implement the system security termination plan, including the security requirements for archiving and disposing of resources.								
Develop the system termination plan to ensure that IT security breaches are avoided during shutdown and long-term protection of archived resources is achieved								
Identify and explain disposition of media and data policies and procedures						✓		
Comply with termination procedures and report any incident or breaches								